UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/066,041	02/01/2002	Don Coppersmith	YOR920020025US1	3936

7590 10/21/2005

IBM CORPORATION
INTELLECTUAL PROPERTY LAW DEPT.
P.O. BOX 218
YORKTOWN HEIGHTS, NY 10598

EXAMINER	
KHOMASSI, NIMA	
ART UNIT	**PAPER NUMBER**
2132	

DATE MAILED: 10/21/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/066,041	COPPERSMITH ET AL.	
	Examiner	Art Unit	
	Nima Khomassi	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *01 February 2002*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *01 February 2002* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

The application having Application No. 10,066,041 has a total of 20 claims pending in the application; there are 5 independent claims and 15 dependent claims, all of which are ready for examination by the Examiner. Claims 1-20 have been examined.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claim 1 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Specifically, the limitation "a number of combination operations" is indefinite.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 1-20 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. The claimed invention manipulate only numbers, abstract concepts or ideas, or signals representing any of the foregoing, the acts are not being applied to appropriate subject matter. Schrader, 22 F.3d at 294-95, 30 USPQ2d at 1458-59. Thus, a process consisting solely of mathematical operations,

i.e., converting one set of numbers into another set of numbers, does not manipulate appropriate subject matter and thus cannot constitute a statutory process.

Also, the claimed invention as a whole must accomplish a practical application. That is, it must produce a "useful, concrete and tangible result." State Street, 149 F.3d at 1373, 47 USPQ2d at 1601-02. Further, patent eligibility standard requires significant functionality to be present to satisfy the useful result aspect of the practical application requirement. See Arrhythmia, 958 F.2d at 1057, 22 USPQ2d at 1036.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-6, 9, 10, 17, 19 and 20 are rejected under 35 U.S.C. 102(b) as being anticipated by Coppersmith et al. (herein referred to as Coppersmith), U.S. Patent No. 5,454,039 (Filed on December 6, 1993, Patented on September 26, 1995).

As per claim 1 and 17, 19 and 20, the computer system, method and computer product for generating a random output stream of bits, the system comprising:
an initial evolving state produced from one or more initial keys (col. 1, line 63-65);
one or more round functions, each round function being part of a step in a sequence of steps, each step applying the respective round function to a current evolving state to produce a respective new evolving state for processing by the next step in the

sequence, the initial evolving state processed by the first step in the sequence (Fig. 1); and one or more mask tables produced from one or more of the initial keys (col. 3, lines 56-59), each of the mask tables having one or more masks, one or more of the masks being combined, in each respective step, with the respective new evolving state in a combination operation to create a respective step output (col. 5, lines 4-7; col. 3, lines 62-65), the random output stream being a concatenation of all the respective step outputs (col. 2, line 6-8; col. 5, line 27-29), and one or more of the masks in the mask tables being replaced by one or more replacement masks after a number of combination operations, the replacement masks not being linear combinations of prior masks (col. 4, lines 50-60; mixing function applied to the masking tables).

As per claim 2, a computer system, as in claim 1, where the number of combination operations before the mask is replaced by the replacement mask is greater than 1 (col. 5, lines 29-35).

As per claim 3, a computer system, as in claim 1, where the number of combination operations before the mask is replaced by the replacement mask is 16 (col. 5, lines 29-35).

As per claim 4, a computer system, as in claim 1, where one or more of the masks is used in more than one of the combination operations before the mask is replaced by the replacement mask (col. 4, lines 50-60).

As per claim 5, a computer system, as in claim 1, where two or more tables are produced from the initial keys (col. 3, lines 56-59) and one or more mask from each table is used in the combination operation (col. 4, lines 50-60).

As per claim 6 and 10, a computer system, as in claim 5 and 9, where the masks from the tables are used in the combination operation in an order (col. 4, lines 50-60).

As per claim 9, a computer system for generating a random output stream of bits, the system comprising: an initial evolving state produced from one or more initial keys (col. 1, lines 63-65); one or more round functions, each round function being part of a step in a sequence of steps, each step applying the respective round function to a current evolving state to produce a respective new evolving state for processing by the next step in the sequence, the initial evolving state processed by the first step in the sequence (Fig. 1); and two or more mask tables produced from one or more of the initial keys (col. 3, lines 56-59), each of the mask tables having one or more masks, one or more of the masks from each table being combined, in each respective step, with the respective new evolving state in a combination operation to create a respective step output (col. 5, lines 4-7; col. 3, lines 62-65), the random output stream being a concatenation of all the respective step outputs (col. 2, line 6-8; col. 5, line 27-29).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claim 7, 8, 11-16, and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Coppersmith as applied to claim 1 above, and further in view of

Smith (herein referred to as Smith), U.S. Patent No. 3,796,830 (Filed on November 2, 1971, Patented on March 12, 1974).

As per claim 7 and 12, Coppersmith teaches the computer system of claim 6 and 9. However, Coppersmith does not explicitly disclose the order of the respective evolving state.

Smith describe: The order is determined by a value of the respective new evolving state (col. 6, lines 58-60). Therefore, it would have been obvious to one of ordinary skill in the computer art at the time the invention was made to combine the computer system of Coppersmith with the substitution output signal method of Smith as determined by the cipher key and message bits to further enhance the cryptographic system.

As per claim 8 and 11, Coppersmith teaches the computer system of claim 5 and 9. However, Coppersmith does not explicitly disclose the combination operation in a lexicographical order. Smith describe: The masks from the tables are used in the combination operation in a lexicographical order (col. 6, lines 43-46). Therefore, it would have been obvious to one of ordinary skill in the computer art at the time the invention was made to combine the computer system of Coppersmith with the non-linear transformation of Smith which includes lexicographical order to further enhance the cryptographic system.

As per claim 13, Coppersmith teaches the computer system of claim 1. However, Coppersmith does not explicitly disclose the non linear permutation of the round function. Smith describe: The round function is a non linear permutation (col. 6, lines 43-46). Therefore, it would have been obvious to one of ordinary skill in the

computer art at the time the invention was made to combine the computer system of Coppersmith with the non-linear permutation of Smith to further enhance the cryptographic system.

As per claim 14, Coppersmith teaches the computer system of claim 13. However, Coppersmith does not explicitly disclose the non-linear permutation to include either a substitution-permutation or Feistel ladder. Smith describe: The non linear permutation includes any one or more of the following: a substitution-permutation network and a Feistel ladder (col. 6, lines 43-46). Therefore, it would have been obvious to one of ordinary skill in the computer art at the time the invention was made to combine the computer system of Coppersmith with the non-linear substitution permutation of Smith to further enhance the cryptographic system.

As per claim 15 and 18, Coppersmith and Smith teaches the computer system of claim 13 and 17. Furthermore, Coppersmith discloses: dividing the current evolving state into a first part and one or more second parts (col. 2, lines 63-64 and col. 3, lines 1-6; mixing function takes the evolving state and divides it into two parts, then the masking function performs the combination operation); applying a first non linear function to the first part to create a first part first result (col. 2, lines 63-64 and col. 3, lines 1-6); applying one or more second non linear functions to the first part to create one or more first part second results (col. 2, lines 63-64 and col. 3, lines 1-6); combining one or more first part second results to one or more of the second parts to create one or more respective interim second parts (col. 2, lines 63-64 and col. 3, lines 1-6); and

concatenating the first part first result and the interim second parts to create a new evolving state (col. 2, lines 6-8).

As per claim 16, Coppersmith and Smith teaches the computer system of claim 13. Furthermore, Coppersmith discloses: dividing the current evolving state into a first part and a second part (col. 2, lines 63-64 and col. 3, lines 1-6; mixing function takes the evolving state and divides it into two parts, then the masking function performs the combination operation); applying a first non linear function to the first part to create a first part first result (col. 2, lines 63-64 and col. 3, lines 1-6); applying a second non linear function to the first part to create a first part second result (col. 2, lines 63-64 and col. 3, lines 1-6); combining the first part second result to the second part to create a respective interim second part (col. 2, lines 63-64 and col. 3, lines 1-6); applying the first non linear function to the interim second part to create a final first result (col. 2, lines 63-64 and col. 3, lines 1-6); applying the second non linear function to the interim second part to create an interim second part second result (col. 2, lines 63-64 and col. 3, lines 1-6); combining the interim second part second result with the first part second result to create a final second result (col. 2, lines 63-64 and col. 3, lines 1-6); and concatenating the final first result and the final second result to create a new evolving state (col. 2, lines 6-8).

Conclusion

Any inquiry concerning this communication or earlier communications should be directed to Nima Khomassi whose telephone number is (571) 272-3775. The examiner can normally be reached Monday-Friday from 8:30 AM to 5:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron Jr., can be reached at (571) 272-3799.

The fax number for Formal or Official faxes to Technology Center 2100 is 571-273-8300. On July 15, 2005, the Central Facsimile (FAX) Number changed from 703-872-9306 to 571-273-8300. As of September 15, 2005, the old number is no longer in service and 571-273-8300 is the only facsimile number recognized for centralized delivery.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have any questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Nima Khomassi
October 17, 2005
Art Unit #2132

GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100